

Approved for use through 10/31/2002 OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1
-------	---

of	1
----	---

Complete if Known	
Application Number	09/654,638
Filing Date	September 5, 2000
First Named Inventor	Tsuyoshi, Takagi
Group Art Unit	To Be Assigned
Examiner Name	To Be Assigned
Attorney Docket Number	13700-0251 (KS#44471/234055)


OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T2
MD	1	HUHNLEIN; <i>A Cryptosystem Based On Non-Maximal Imaginary Quadratic Orders With Fast Decryption</i> ; ADVANCES IN CRYPTOLOGY-EUROCRYPT '98, 1998, PGS 294-307	✓
MD	2	MENEZES; <i>Handbook of Applied Cryptography</i> ; 1997, CRC Press, Boca Raton, Florida 33431	✗
MD	3	BUCHMANN; <i>On the Complexity and Efficiency of a New Key Exchange System</i> ; ADVANCES IN CRYPTOLOGY - EUROCRYPT '89; 1990, pgs 597-616	✓
MD	4	BIEHL; <i>Cryptographic Protocols Based on Discrete Logarithms in Real-Quadratic Orders</i> ; ADVANCES IN CRYPTOLOGY - CRYPTO '94, 1994, pgs. 56-60	
MD	5	RIVEST; <i>Obtaining Digital Signatures and Public-Key Cryptosystems</i> ; Communications of the ACM, Feb. 1978, Vol. 21, #2, pgs. 120-126.	
MD	6	CHAUM; <i>Centre for Mathematics and Computer Science</i> , 1998, Springer-Verlag, pgs. 212-214.	
MD	7	GENNARO; <i>RSA-Based Undeniable Signatures</i> ; 1998, Springer-Verlag, pgs. 132, 149.	
MD	8	SHANKS; <i>On Gauss and Composition 1</i> , NUMBER THEORY AND APPLICATIONS, pgs. 163-204, 1989, Kluwer Academic Publishers	
MD	9	<i>A Cryptosystem Based on Non-Maximal Imaginary Quadratic Orders with Fast Decryption</i> ; Proceedings Eurocrypt '98; March 1998, pgs. 294-307.	
MD	10	<i>Conference on the Mathematics of Public Key Cryptography</i> ; June 12, 1999, pgs 1-17	

RECEIVED

MAR 28 2001

Technology Center 2100

Examiner Signature		Date Considered	2/14/04
-----------------------	---	--------------------	---------

¹Unique citation designation number. ²Applicant is to place a check mark here if English language translation is attached.

BEST AVAILABLE COPY